b.) Remarks

Claims 1-58 are pending in this application. Claim 1 has been amended in various particulars as indicated hereinabove. New Claim 58 has been added to alternatively define Applicants' invention.

Claims 1-2, 5-15, 18-28, 31-41, 46-50, and 55-57 were rejected under 35 U.S.C. 103(a) as being unpatentable over Shannon (U.S. Pat. No. 6,233,618) in view of Munger et al. (U.S. Pat. No. 6,834,310). In a related rejection, claims 3-4, 16-17, 29-30, 42-45 and 51-54 were rejected under 35 U.S.C. 103(a) as being unpatentable over Shannon in view of Trcka et al. (U.S. Pat. No. 6,453,345) and Munger et al. These rejections are respectfully traversed for the following reasons.

Some background for the applied references may be helpful to understanding the differences between the present claimed invention and the systems disclosed in the references.

A denial service attack is a form of internet attack in which large volumes of undesirable network traffic, often packets carrying no information, are directed at a target network device, such as a web server, in order to undermine the operation of the target device by overwhelming the target device with network traffic. In short, the target network device becomes so concerned with handling the flood of invalid or meaningless packets, that it can no longer perform its fundamental task of responding to valid packets to provide its intended services.

The present invention is different then solutions, and also those of the applied references. Specifically, it is directed to insuring that a network domain is not sourcing this undesirable, denial of service attack, network traffic. Claim 1, for example, is directed to a network domain including a routing device handling traffic into and out of the network domain. A monitor/regulator is then provided that monitors this first routing device. It determines if the first network domain is sourcing undesirable network traffic. New claim 58 has similar features. That is, the claimed systems determine whether there

is some device within the network domain that is creating this undesirable network traffic directed at a target network device.

Claim 2 further characterizes this invention of claim 1. Specifically, it describes that the monitor/regulator makes its determination based on the differential characteristics of network traffic routed out of the network domain and network traffic routed into the network domain. It looks at, for example, if a much higher volume of traffic is leaving the domain rather than being routed into the domain. It uses this as a mechanism for determining if the network domain is the source of this undesirable network traffic.

Claim 40 further adds that the monitor/regulator monitors flows and determines whether the network domain is sourcing undesirable network traffic based on these flows. The monitor/regulator monitors the flows including tracking source and destination addresses and port information, as further described in claim 41.

Claim 42 describes that the monitor/regulator generates statistics concerning destination addresses and then determines whether first network domain is sourcing undesirable network traffic based on these statistics.

Claim 43 describes that the lengths of packets are used to determine whether the network domain is sourcing undesirable network traffic.

Claim 44 describes that the time to live values are used to determine whether there is undesirable network traffic.

Claim 45 describes that the monitor/regulator tracks differences between outbound transmission control protocol (TCP) synchronize (SYN) and finish (FIN) packets and inbound response packets and determines whether or not the first network domain is sourcing undesirable network traffic.

Claim 46 further adds that the monitor/regulator instructs a routing device to lower priority of the undesirable network traffic.

Claim 47 describes that the monitor/regulator instructs a routing device to slow the undesirable network traffic.

The invention of claim 1 is different from that disclosed in the applied references such as the Shannon patent. Specifically, the Shannon patent is directed to a different problem. The Shannon patent is directed to protecting its domain, the network region under control. Specifically, as described in the Shannon patent at column 3, beginning at line 45, for example, the "network device" is responsible for controlling access by client computers to data available from server computers. Typically, the device monitors a network domain and specifically attempts by client computers in that network domain to access information, such as web pages, uniform resource locators (URL's), for example. The system looks at addresses of the client's making the request. The device may then block access to, for example, pornography, if there is some policy against that client accessing that type of content. In short, the Shannon patent is directed to a different problem--controlling access by a number of clients to certain content on the internet.

In contradistinction, claim 1, for example, is directed to determining whether a network domain is the source of undesirable network traffic, that is, a flood of network traffic associated with a denial of service attack. In one sense, the present invention is not directed to protecting its domain as the Shannon system, but instead ensures that its domain is not the source of an attack on some other target network device.

The Munger et al. patent is relevant insofar as it mentions denial of service attacks. See abstract of the Munger et al. patent. Similar to the Shannon patent, however, the Munger et al. patent does not deal with or have a solution to the problem addressed by the present claimed invention. Generally the Munger patent is directed to certain routing protocol (termed tunneled agile routing protocol). This is a technique by which a packet's true destination can be concealed behind a layer of encryption generated using a link key. See Munger patent at column 3, beginning at line 18.

Of relevance to the pending claims is the fact that the Munger patent does not show or suggest monitoring network traffic routed by a routing device of a network domain to determine if that network domain is sourcing undesirable network traffic.

In fact, like the Shannon patent, the Munger system does not offer any means for ensuring that a monitored domain is the source of a denial of service attack.

For example, at column 29, beginning at line 37, Munger patent mentions the saturation that occurs in a denial of service attack. This discussion, however, is directed at protecting the target network device at the target network device from this flood. In contradistinction, it does not mention protecting the target network device at the source as described in claim 1 for example.

Thus, Applicants believe that the claimed invention is distinguishable over the applied references.

Applicants believe that the present application is in condition for allowance. A Notice of Allowance is respectfully solicited. Should any questions arise, the Examiner is encouraged to contact the undersigned.

Respectfully submitted,

By _____
J. Grant Houston
Registration No.: 35,900
Tel.: 781 863 9991
Fax: 781 863 9931

Lexington, Massachusetts 02421
Date: December 12, 2005